State of West Virginia Office of Technology

Policy: Removable Media

Issued by the CTO

Procedure No: WVOT-PO1011 Issue Date: 08.19.09 Revised: Page 1 of 9

1.0 PURPOSE

This policy will define standards, procedures, and restrictions for Executive Branch employees who use State-owned and authorized removable media to connect to the West Virginia Office of Technology (WVOT) network in order to store, back-up, relocate, or otherwise access enterprise data in a safe, secure manner.

The security safeguards may vary by device type, but in all cases must comply with the requirements set forth in this policy. This document is not all-inclusive and management has the authority and discretion to appropriately address any unacceptable behavior and/or practice not specifically mentioned herein.

2.0 SCOPE

This policy applies to all Departments (including Agencies, Boards, and Commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. However, the WVOT recommends that all agencies, including those excluded above, follow this procedure.

3.0 BACKGROUND

Under the provisions of West Virginia Code 5A-6-4a, the Chief Technology Officer (CTO) is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

This policy is one in a series of IT related policies intended to define and enable the incorporation of appropriate practices into all activities using technology in the State of West Virginia.

4.0 RELEVANT DOCUMENTS/MATERIAL

4.1 WVOT-PO1001 – Information Security Policy

4.2 WVOT-PO1002 – Acceptable Use of State-Provided Wireless Devices

4.3 WVOT-PO1004 – Acceptable Use of Portable Devices

4.4 WVOT Web Site Home Page - IT Security Web Policies Issued by the Chief Technology Officer (CTO).

4.5 West Virginia Code §5A-6-4a Controls – “Duties of the Chief Technology Officer Relating to Security of Government Information”

5.0 RESPONSIBILITY/REQUIREMENTS

5.1 This removable media policy pertains to, but is not limited to all devices and accompanying media that fit the following criteria:

- Portable USB-based flash drives, also known as thumb drives, jump drives, or key drives;
- Memory cards in SD, CompactFlash, Memory Stick or any related flash-based supplemental storage media;
- USB card readers that allow connectivity to a PC;
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function;
- PDAs, cell phones, and Smartphones with internal flash or hard drive-based memory that support a data storage function;
- Digital cameras with internal or external memory support;

- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks;

- Any hardware that provides connectivity to USB devices through means such as wireless or wired network access; and

- Any applicable emerging technologies.

5.2 Only minimal personal use of State-provided IT resources is permitted, and should not interfere with the legitimate business of the State. (See WVOT-PO1001 – *State of West Virginia Information Security Policy, Appendix A.*)

5.3 The WVOT reserves the right to refuse the ability to connect removable media and USB devices to the State network if such media is being used in such a way that puts the State's systems, data, users, and customers at risk.

5.4 The WVOT will establish audit trails or logs in all situations it feels warranted. Such trails will be able to track the attachment of external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The WVOT has the right to monitor all employee access and/or connection to the State network in order to identify and analyze unusual usage patterns or other activity.

5.5 Agencies may prohibit flash drive use at any time in order to protect data. This prohibition should be implemented through policy, training, and/or use of technical controls (e.g. port blocking control).

5.6 To maintain protection against threats and to protect sensitive data, employees **must** use WVOT-approved removable media and comply with the following standards:

5.6.1 All removable media, if intended to contain legally protected data, must be preloaded with WVOT-approved password and encryption software, where available;

5.6.2 Removable media may only be used to transport State business data;

5.6.3 Employees may not copy sensitive State data onto personal devices;

5.6.4 Employees may not use removable media devices for long term data storage.

5.6.4.1 For security purposes, State data should not be stored on removable media. Users must store all data on State servers or storage (e.g. home directory or shared network drives, etc.). If in doubt, contact the WVOT Service Desk.

5.6.4.2 If a State network connection is unavailable (ex: offsite use), removable media may be used for short term data storage and back-up purposes.

5.7 Employees are prohibited from using flash drives or portable media that do not have adequate protection mechanisms to store or transmit sensitive data (e.g., Protected Health Information {PHI} or sensitive Personally Identifiable Information {PII}).

5.8 Employees must not uninstall or de-activate any security controls loaded onto the media device by the WVOT

5.9 Removable media must be physically protected against loss, damage, abuse, or misuse when used, stored, and in transit.

5.10 Employees will contact an immediate supervisor and/or the Chief Information Security Officer (CISO) if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting must occur up the supervisory or management chain without delay.

5.11 Employees must immediately report all security incidents or suspected incidents of unauthorized data access, data loss, and/or disclosure to the CTO, the CISO, and/or the WVOT Service Desk.

6.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based on recommendations of the WVOT and the West Virginia Division of Personnel

7.0 DEFINITIONS

7.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

7.2 Chief Information Security Officer (CISO) – Person designated by the CTO to oversee Information Security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

7.3 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

7.4 Legally Protected – Personally identifiable information of any kind, such as personal, financial, academic, or health related data, which is protected by privacy and/or security laws. Laws are divided into categories, federal and state, which govern the handling of certain types of sensitive information that must be protected by those authorized to use it.

7.5 Personally Identifiable Information (PII) –Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.

7.6 Protected Health Information (PHI) – Information, including demographic data, that relates to: an individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. PHI includes many common identifiers (e.g., name, address, birth date, Social Security Number).

7.7 Removable Media – Storage media which can be removed from its reader device, conferring portability on the data it carries.

7.8 Security Incident – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

7.9 West Virginia Division of Personnel – A division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq*., which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

7.10 West Virginia Office of Technology (WVOT)- The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq*., which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

8.0 LEGAL AUTHORITY (See West Virginia Code §5A-6-1 *et seq*.)

The CTO is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO has authority to issue policies, procedures, and standards to accomplish this mission. This policy will apply across the Executive Branch, with the exclusion of the West Virginia State Police, the Division of Homeland Security and Emergency Management, any constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than Information Security policies issued by the WVOT the more restrictive provisions will prevail.

9.0 INDEX